Gustavo Ponce, Esq.
Nevada Bar No. 15084
Mona Amini, Esq.
Nevada Bar No. 15381
KAZEROUNI LAW GROUP, APC
6787 W. Tropicana Avenue, Suite 250
Las Vegas, Nevada 89103
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
E-mail: gustavo@kazlg.com
mona@kazlg.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

L.G., a minor by and through Guardian ad Litem, FESETO BROUGHTON-GREGG, individually and on behalf of all others similarly situated,

Plaintiff,

vs.

PERRY JOHNSON & ASSOCIATES, INC.; AND NORTHWELL HEALTH, INC.,

Defendants.

Case No.: 2:23-cv-01987

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

//

//

//

//

//

//

//

INTRODUCTION

1. Plaintiff L.G., a minor by and through Guardian ad Litem, FESETO BROUGHTON-GREGG, individually and on behalf of all others similarly situated ("Plaintiff"), individually, and on behalf of all others similarly situated (collectively, the "Class members") brings this class action against Defendants PERRY JOHNSON & ASSOCIATES, INC. ("PJ&A") and NORTHWELL HEALTH, INC. ("Northwell") (jointly as "Defendants"), for their failure to secure and safeguard his and approximately 3.9 million similarly situated Class members' personally identifying information ("PII") and personal health information ("PHI"), including but not limited to their names, Social Security numbers, dates of birth, addresses, medical record numbers, encounter numbers, medical information, and dates/times of service.

2. PJ&A is a third-party vendor of health information technology solutions used by Northwell, which is the largest health system in New York.

3. Between approximately March 27, 2023, and May 2, 2023, an unauthorized third party gained access to PJ&A's network system and obtained files containing information about Northwell's current and former patients, including Plaintiff and the Class (the "Data Breach").

4. Defendants owed a duty to Plaintiff and Class members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their PII/PHI against unauthorized access and disclosure. Defendants breached that duty by, among other things, failing to implement and maintain reasonable security procedures and practices to protect Plaintiff and other similarly situated Northwell patients' PII/PHI from unauthorized access and disclosure.

5. As a result of Defendants' inadequate data security and breach of their duties and obligations, the Data Breach occurred, and Plaintiff's and Class members' PII/PHI was accessed and disclosed. This action seeks to remedy these failings and their consequences. Plaintiff brings this action on behalf of himself and all persons whose PII/PHI was exposed as a result of the Data Breach, which occurred between approximately March 27, 2023, and May 2, 2023.

6. Plaintiff, on behalf of himself and all other Class members, asserts claims for negligence, including negligence per se, breach of implied contract, unjust enrichment, and

seeks declaratory relief, injunctive relief, monetary damages, statutory damages, punitive damages, equitable relief, and all other relief authorized by law.

JURISDICTION AND VENUE

7. This Court has subject matter of this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs, and there are more than 100 members in the proposed Class, and at least one member of the Class is a citizen of a state different from Defendants.

8. This Court has personal jurisdiction over Defendant Perry Johnson & Associates, Inc. because it is a corporation incorporated under the laws of the State of Nevada, has its principal place of business in the State of Nevada, and regularly conducts business within this district.

9. This Court has personal jurisdiction over Defendant Northwell Health, Inc., because it transacts business within this state and makes or performs contracts within this state, including its business association and contracts with Defendant Perry Johnson & Associates, Inc.

PARTIES

10. Plaintiff L.G. is a citizen of the State of New York.

11. Plaintiff obtained healthcare or related services from Northwell. As a condition of receiving services, Northwell required Plaintiff to provide them with his PII/PHI.

12. Based on representations made by Northwell, and Plaintiff's reliance on such representations, Plaintiff believed Northwell had implemented and maintained reasonable security and practices to protect his PII/PHI. Relying on Northwell's representations and his belief that his PII/PHI would be reasonably safeguarded, Plaintiff provided his PII/PHI to Northwell in connection with receiving healthcare services.

13. Plaintiff takes great care to protect his PII/PHI. If Plaintiff had known that Northwell does not adequately protect the PII/PHI in its possession, including by contracting with companies that do not adequately protect the PII/PHI in their possession, he would not have agreed to entrust Northwell with his PII/PHI or obtained healthcare services from Northwell.

14. On or around November 3, 2023, Plaintiff received a "NOTICE OF DATA BREACH" letter from Defendants informing Plaintiff that between March 27, 2023 and May 2, 2023, an unauthorized party had accessed and downloaded certain files from PJ&A's systems, which impacted Plaintiff's PII/PHI data entrusted to Northwell, including Plaintiff's name, date of birth, address, medical record number, hospital account number, and clinical information such as the name of the treatment facility, the name of Plaintiff's healthcare providers, Plaintiff's admission diagnosis and Plaintiff's date(s) and time(s) of service.

15. As a direct result of the Data Breach, Plaintiff has suffered injury and damages including, *inter alia*, a substantial and imminent risk of identity theft and medical identity theft; the wrongful disclosure and loss of confidentiality of his highly sensitive PII/PHI; deprivation of the value of his PII/PHI; and overpayment for services that did not include adequate data security.

16. Defendant Perry Johnson & Associates, Inc.is a Nevada corporation with its principal place of business at 1489 W Warm Springs Rd., Henderson, Nevada 89014.

17. Defendant Northwell Health, Inc. is a New York not-for-profit corporation with its principal place of business at 2000 Marcus Ave., New Hyde Park, New York 11042.

FACTUAL ALLEGATIONS

PII/PHI Is a Valuable Property Right that Must Be Protected

18. In a Federal Trade Commission ("FTC") roundtable presentation, former Commissioner, Pamela Jones Harbour, underscored the property value attributed to PII by observing:

> Most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency. The larger the data set, the greater potential for analysis – and profit.[1]

19. The value of PII as a commodity is measurable. "PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of

[1] FTC, *Statement of FTC Commissioner Pamela Jones Harbour* (Remarks Before FTC Exploring Privacy Roundtable) (Dec. 7, 2009), https://www.ftc.gov/public-statements/2009/12/remarks-ftc-exploring-privacy-roundtable.

traditional financial assets."[2] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market" for several years.

20. Companies recognize PII as an extremely valuable commodity akin to a form of personal property. For example, Symantec Corporation's Norton brand has created a software application that values a person's identity on the black market.[3]

21. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals openly post credit card numbers, Social Security numbers, PII and other sensitive information directly on various illicit Internet websites making the information publicly available for other criminals to take and use. This information from various breaches, including the information exposed in the Data Breach, can be aggregated and become more valuable to thieves and more damaging to victims. In one study, researchers found hundreds of websites displaying stolen PII and other sensitive information. Strikingly, none of these websites were blocked by Google's safeguard filtering mechanism – the "Safe Browsing list."

22. Recognizing the high value that consumers place on their PII, some companies now offer consumers an opportunity to sell this information to advertisers and other third parties. The idea is to give consumers more power and control over the type of information they share – and who ultimately receives that information. By making the transaction transparent, consumers will make a profit from the surrender of their PII.[4] This business has created a new market for the sale and purchase of this valuable data.[5]

23. Consumers place a high value not only on their PII, but also on the privacy of that data. Researchers shed light on how much consumers value their data privacy – and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and

---

[2] *See* Soma, *Corporate Privacy Trend, supra*.

[3] Risk Assessment Tool, Norton 2010, www.everyclickmatters.com/victim/assessment-tool.html.

[4] Steve Lohr, *You Want My Personal Data? Reward Me for It*, N.Y. Times (July 16, 2010) *available at* https://www.nytimes.com/2010/07/18/business/ 18unboxed.html.

[5] *See* Julia Angwin and Emil Steel, *Web's Hot New Commodity: Privacy*, Wall Street Journal (Feb. 28, 2011) *available at* https://www.wsj.com/articles/SB10001424052748703529004576160764037920274.

accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[6]

24. One study on website privacy determined that U.S. consumers valued the restriction of improper access to their PII between $11.33 and $16.58 per website.[7]

25. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

Theft of PII/PHI Has Grave and Lasting Consequences for Victims

26. A data breach is an incident in which sensitive, protected, or confidential data has potentially been viewed, stolen, or used by an individual unauthorized to do so. As more consumers rely on the internet and apps on their phone and other devices to conduct every-day transactions, data breaches are becoming increasingly more harmful.

27. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identity thieves use PII to take over existing financial accounts, open new financial accounts, receive government benefits and incur charges and credit in a person's name.[8] As the GAO Report states, this type of identity theft is so harmful because it may take time for the victim to become aware of the theft and can adversely impact the victim's credit rating.

28. In addition, the GAO Report states that victims of identity theft will face "substantial costs and inconveniences repairing damage to their credit records … [and their] good name." According to the FTC, identity theft victims must spend countless hours and large amounts of money repairing the impact to their good name and credit record.[9]

---

[6] Janice Y. Tsai, et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study Information Systems Research* 22(2) 254, 254 (June 2011), *available at* https://www.jstor.org/stable/23015560?seq=1#

[7] II–Horn, Hann, et al., *The Value of Online Information Privacy: An Empirical Investigation* (Mar. 2003) at table 3, *available at* https://ideas.repec.org/p/wpa/wuwpio/0304001.html (emphasis added).

[8] *See* GAO, GAO Report 9 (2007) *available at* http:///www.gao.gov/new.items/d07737.pdf.

[9] *See* FTC Identity Theft Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

29. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.[10] According to Experian, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan; change a billing address so the victim no longer receives bills; open new utilities; obtain a mobile phone; open a bank account and write bad checks; use a debit card number to withdraw funds; obtain a new driver's license or ID; use the victim's information in the event of arrest or court action.[11]

30. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

31. According to the IBM and Ponemon Institute's 2019 "Cost of a Data Breach" report, the average cost of a data breach per consumer was $150 per record.[13] Other estimates have placed

---

[10] The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 C.F.R. § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer, or taxpayer identification number." *Id.*

[11] *See* Susan Henson, *What Can Identity Thieves Do with Your Personal Information and How Can You Protect Yourself?*, EXPERIAN (Sept. 7, 2017), *available at* https://www.experian.com/blogs/ask-experian/what-can-identity-thieves-do-with-your-personal-information-and-how-can-you-protect-yourself/.

[12] Brian Naylor, Victims of Social Security Number Theft Find It's Hard to Bounce Back, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying- about-identity-theft.

[13] Brook, *What's the Cost of a Data Breach in 2019*, *supra*.

the costs even higher. The 2013 Norton Report estimated that the average cost per victim of identity theft – a common result of data breaches – was $298 dollars.[14] And in 2019, Javelin Strategy & Research compiled consumer complaints from the FTC and indicated that the median out-of-pocket cost to consumers for identity theft was $375.[15]

32. A person whose PII has been compromised may not see any signs of identity theft for years. According to the GAO Report:

> "[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."

33. For example, in 2012, hackers gained access to LinkedIn's users' passwords. However, it was not until May 2016, four years after the breach, that hackers released the stolen email and password combinations.[16]

34. PHI is particularly valuable and has been referred to as a "treasure trove for criminals."[17] A cybercriminal who steals a person's PHI can end up with as many as "seven to ten personal identifying characteristics of an individual."[18]

35. All-inclusive health insurance dossiers containing sensitive health insurance information, names, addresses, telephone numbers, email addresses, SSNs, and bank account information, complete with account and routing numbers, can fetch up to $1,200 to $1,300 each on the black market.[19]

---

[14] Norton By Symantec, 2013 Norton Report 8 (2013), *available at* https://yle.fi/tvuutiset/uutiset/upics/liitetiedostot/norton_raportti.pdf.

[15] Facts + Statistics: *Identity Theft and Cybercrime*, Insurance Information Institute, *available at* https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (citing the Javelin report).

[16] *See* Cory Scott, *Protecting Our Members*, LINKEDIN (May 18, 2016), *available at* https://blog.linkedin.com/2016/05/18/protecting-our-members.

[17] *See* Andrew Steager, *What Happens to Stolen Healthcare Data*, HEALTHTECH MAG. (Oct. 20, 2019) https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon

[18] *Id.*

[19] *See* SC Staff, *Health Insurance Credentials Fetch High Prices in the Online Black Market*, SC MAG. (July 16, 2013), https://www.scmagazine.com/news/breach/health-insurance-credentials-fetch-high-prices- in-the-online-black-market.

36. According to a report released by the Federal Bureau of Investigation's ("FBI") Cyber Division, criminals can sell healthcare records for 50 times the price of a stolen Social Security or credit card number.[20]

37. It is within this context that Plaintiff and thousands of similar individuals must now live with the knowledge that their PII/PHI is forever in cyberspace, putting them at imminent and continuing risk of damages, and was taken by unauthorized persons willing to use the information for any number of improper purposes and scams, including making the information available for sale on the dark web and/or the black market.

Defendants and their Collection of PII/PHI

38. Upon information and belief, PJ&A "provides medical transcription services to various healthcare organizations," including Northwell.[21]

39. Upon information and belief, Northwell used PJ&A for medical transcription and dictation services.[22]

40. Plaintiff and Class members are current or former patients of Northwell and entrusted Northwell with their PII/PHI, including but not limited to the PII/PHI compromised by the Data Breach.

The Data Breach

41. Between approximately March 27, 2023, and May 2, 2023, "An unauthorized party gained access to the PJ&A network . . . and, during that time, acquired copies of certain files from PJ&A systems."[23]

42. According to the "Cyber Incident Notice" posted on PJ&A website,[24] the PII/PHI affected in the Data Breach compromised the names, dates of birth, addresses, medical record

---

[20] *See* Federal Bureau of Investigation, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain* (April 8, 2014), https://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf.
[21] https://www.pjats.com/downloads/Notice.pdf
[22] https://longisland.news12.com/northwell-health-vendor-patient-information-may-have-been-impacted-by-data-breach.
[23] https://www.pjats.com/downloads/Notice.pdf
[24] *Id.*

numbers, hospital account numbers, admission diagnoses, dates and times of service, Social Security numbers, insurance information, clinical information such as laboratory and diagnostic testing results, medications, treatment facility names, and healthcare provider names, of Plaintiff and the Class members.

43. Northwell's Notice of Privacy Practices states, "You have a right to be notified in the event of a breach of the privacy of your unsecured protected health information by Northwell Health or its business associates;" and promises that they "will be notified as soon as reasonably possible, but no later than 60 days following our discovery of the breach."[25]

44. PJ&A informed Northwell of the Data Breach on July 21, 2023; however, Defendants failed to notify Plaintiff and the Class members until early November 2023, over three months after their knowledge of the Data Breach.

45. Defendants' failure to promptly notify Plaintiff and Class members that their PII/PHI was accessed and stolen by unauthorized third parties allowed those who were able to obtain their PII/PHI to monetize, misuse, or disseminate that PII/PHI before Plaintiff and Class members could take affirmative steps to protect their sensitive information. As a result, Plaintiff and the Class members have and will continue to suffer indefinitely from the damage of substantial, imminent, and concrete risk that their identities will be, or already have been, stolen and misused by unauthorized third parties.

46. As a result of the Data Breach and Defendants' conduct and/or omissions, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantially increased and imminent risk of identity theft; (ii) the unauthorized disclosure and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with efforts attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and

[25] https://www.northwell.edu/sites/northwell.edu/files/2023-09/notice-of-privacy-practices-english-23.pdf

money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for services that were received without adequate data security to reasonably safeguard Plaintiff and the Class members' PII/PHI from unauthorized disclosure, access, and exfiltration.

CLASS ACTION ALLEGATIONS

47. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff seeks to represent and intends to seek certification of a class (the "Class") defined as:

> All individuals whose PII/PHI was subjected to the Data Breach, including all individuals who were sent a notice of the Data Breach by Defendants.

48. Excluded from the Class are: (1) Defendants and their respective officers, directors, employees, principals, affiliated entities, controlling entities, agents, and other affiliates; (2) the agents, affiliates, legal representatives, heirs, attorneys at law, attorneys in fact, or assignees of such persons or entities described herein; and (3) the Judge(s) assigned to this case and any members of their immediate families.

49. Certification of Plaintiff's claims for class wide treatment is appropriate because Plaintiff can prove the elements of their claims on a class wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

50. The Class members are so numerous and geographically dispersed throughout California that joinder of all Class members would be impracticable. While the exact number of Class members is unknown, based on information and belief, the Class consists of tens of thousands of individuals, including Plaintiff and the Class members. Plaintiff therefore believe that the Class is so numerous that joinder of all members is impractical.

51. Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had their PII compromised in the Data Breach. Plaintiff and Class members were injured by the same wrongful acts, practices, and omissions committed by Defendants, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class members.

52. There is a well-defined community of interest in the common questions of law and fact affecting Class members. The questions of law and fact common to Class members predominate over questions affecting only individual Class members, and include without limitation:

a) Whether Defendants had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII/PHI it collected, stored, and maintained from Plaintiff and Class members;

b) Whether Defendants had duties not to disclose the PII/PHI of Plaintiff and Class members to unauthorized third parties;

c) Whether Defendants failed to exercise reasonable care to secure and safeguard Plaintiff's and Class members' PII/PHI;

d) Whether Defendants breached their duty to protect the PII/PHI of Plaintiff and each Class member; and

e) Whether Plaintiff and each Class member are entitled to damages and other equitable relief.

53. Plaintiff will fairly and adequately protect the interests of the Class members. Plaintiff is an adequate representatives of the Class in that Plaintiff have no interests adverse to or that conflicts with the Class Plaintiff seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection and consumer privacy class actions of this nature.

54. A class action is superior to any other available method for the fair and efficient adjudication of this controversy since individual joinder of all Class members is impractical. Furthermore, the expenses and burden of individual litigation would make it difficult or impossible for the individual members of the Class to redress the wrongs done to them, especially given that the damages or injuries suffered by each individual member of the Class are outweighed by the costs of suit. Even if the Class members could afford individualized litigation, the cost to the court system would be substantial and individual actions would also present the potential for inconsistent

or contradictory judgments. By contrast, a class action presents fewer management difficulties and provides the benefits of single adjudication and comprehensive supervision by a single court.

55. Defendants have acted or refused to act on grounds generally applicable to the entire Class, thereby making it appropriate for this Court to grant final injunctive, including public injunctive relief, and declaratory relief with respect to the Class as a whole.

CAUSES OF ACTION

COUNT I

NEGLIGENCE

56. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

57. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting the PII/PHI in their possession, custody, or control.

58. In addition, Defendants' duties arise from, *inter alia*, the HIPAA Privacy Rule ("Standards for Privacy of Individually Identifiable Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and E, and the HIPAA Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C (collectively, "HIPAA Privacy and Security Rules"). Defendants' duties also arise from Section 5 of the FTC Act ("FTCA"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by business, such as Defendants, of failing to employ reasonable measures to protect and secure Plaintiff and the Class members' PII/PHI.

59. Defendants' violation of the HIPAA Privacy and Security Rules and Section 5 of the FTCA constitutes negligence *per se*.

60. Defendants knew or should have known the risks of collecting and storing Plaintiff's and all other Class members' PII/PHI and the importance of maintaining secure systems. Defendants knew or should have known of the many data breaches that targeted healthcare provides that collect and store PII/PHI in recent years.

61. Given the nature of Defendants' businesses, the sensitivity and value of the PII/PHI they maintain, and the resources at their disposal, Defendants should have identified the vulnerabilities to their systems or their third-party vendor's systems and prevented the Data Breach from occurring.

62. Defendants breached these duties by failing to, or contracting with companies that failed to, exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect PII/PHI entrusted to it—including Plaintiff's and Class members' PII/PHI.

63. It was reasonably foreseeable for Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class members' PII/PHI by failing to, or contracting with companies that failed to, design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class members' PII/PHI to unauthorized individuals.

64. As a result of Defendants' above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and Class members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII/PHI which remains in Defendants' possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII/PHI compromised as a result of the Data Breach; and (vii) overpayment for the services that were received without adequate data security measures implemented by Defendants.

COUNT II

BREACH OF IMPLIED CONTRACT

65. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

66. In connection with receiving healthcare services, Plaintiff and all other Class members entered into implied contracts with Northwell, who contracted with PJ&A.

67. Plaintiff and Class members paid money to Northwell, directly or through their insurance, and provided Northwell with their PII/PHI pursuant to said implied contracts. In exchange, Northwell agreed, and Plaintiff and Class members understood, that among other things, Northwell would: (1) provide services to Plaintiff and Class members; (2) take reasonable measures to protect the security and confidentiality of Plaintiff's and Class members' PII/PHI; and (3) safeguard Plaintiff's and Class members' PII/PHI in compliance with state and federal laws, regulations, and industry standards.

68. The protection of PII/PHI was a material term of the implied contracts between Plaintiff and Class members, on the one hand, and Northwell, on the other hand. Indeed, as set forth supra, Northwell recognized the importance of data security and the privacy of Northwell's patients' PII/PHI.

69. Had Plaintiff and Class members known that Northwell would not adequately protect their PII/PHI, they would not have agreed to provide their PII/PHI to Northwell or received healthcare or other services from Northwell, which they were required to pay for and Northwell received compensation for in return.

70. Plaintiff and Class members performed their obligations under the implied contract when they provided Northwell with their PII/PHI and paid for healthcare or other services from Northwell.

71. Northwell breached its implied contracts with Plaintiff and the Class members in failing to implement and maintain reasonable security measures to protect and safeguard their PII/PHI, including by ensuring companies it contracts with implement and maintain reasonable

security measures to protect PII/PHI, and in failing to implement and maintain security protocols and procedures to protect Plaintiff's and Class members' PII/PHI in a manner complying with applicable state and federal laws, regulations, and industry standards.

72. Northwell's breach of its obligations of its implied contracts with Plaintiff and Class members directly resulted in the Data Breach and the injuries that Plaintiff and all other Class members have suffered from the Data Breach.

73. Plaintiff and all other Class members were damaged by Northwell's breach of implied contracts because: (i) they paid—directly or through their insurers—for data security protection they did not receive; (ii) they face a substantially increased risk of identity theft and medical theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (iii) their PII/PHI was improperly disclosed to unauthorized individuals; (iv) the confidentiality of their PII/PHI has been breached; (v) they were deprived of the value of their PII/PHI, for which there is a well-established national and international market; (vi) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) overpayment for services that were received without adequate data security.

COUNT III

UNJUST ENRICHMENT

74. Plaintiff realleges and incorporates by reference all proceeding paragraphs as if fully set forth herein.

75. Defendants received a monetary benefit from Plaintiff and the Class members in the form of monies paid to Northwell for healthcare services, which Northwell used in turn to pay for PJ&A's services, and which was centered around Plaintiff and the Class members providing their PII/PHI in order to receive such healthcare services.

76. Defendants accepted and/or had knowledge of the benefits conferred upon them by Plaintiff and Class members; and Defendants both benefitted from the receipt of Plaintiff's and Class members' PII/PHI, as it was used in the course of PJ&A's services provided to Northwell.

77. As a result of Defendants' conduct, Plaintiff and Class members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy and security practices and procedures that Plaintiff and Class members paid for without reasonable data privacy and security practices and procedures that they received.

78. Plaintiff and the Class members would remain injured and Defendants would be unjustly enriched if they were permitted to retain money belonging to Plaintiff and the Class members because Defendants failed to adequately implement the data privacy and security procedures that Plaintiff and Class members paid for and that were otherwise required pursuant to state and federal laws, regulations, and industry standards.

79. Defendants should be disgorged of all unlawful proceeds received by them from Plaintiff and the Class members in light of their unlawful conduct and Data Breach caused by their inadequate data security.

80. Plaintiff and the Class members are entitled to equitable relief as they have no adequate remedy at law for their injuries suffered, and continuing to accrue, as a result of Defendants' unlawful conduct and Data Breach caused by their inadequate data security.

PRAYER FOR RELIEF

81. Plaintiff, individually and on behalf of the Class, respectfully requests that (i) this action be certified as a class action, (ii) Plaintiff be designated a representative of the Class, (iii) Plaintiff's counsel be appointed as counsel for the Class.

82. Plaintiff, individually and on behalf of the Class, further requests that upon final trial or hearing, judgment be awarded against Defendants as follows:

- actual and punitive damages to be determined by the trier of fact;
- equitable relief, including restitution, as may be appropriate;
- injunctive relief, including remedial measures to be implemented by Defendants designed to prevent such a data breach by adopting improved data security practices necessary to safeguard Plaintiff and the Class members' PII/PHI and

extended identity theft protection and credit monitoring services design o protect Plaintiff and the Class members from identity theft and fraud;

- declaratory relief, as may be appropriate;
- pre- and post-judgment interest at the applicable legal rates;
- attorneys' fees, litigation expenses, and costs of suit; and
- any such other and further relief the Court deems just and proper.

DEMAND FOR JURY TRIAL

83. Plaintiff hereby demands a jury trial on all issues so triable.

DATED this 30th day of November 2023.

Respectfully submitted,

KAZEROUNI LAW GROUP, APC

By: */s/ Mona Amini*
Gustavo Ponce, Esq.
Mona Amini, Esq.
6787 W. Tropicana Ave., Suite 250
Las Vegas, Nevada 89103

Attorneys for Plaintiff